



1 **GÉANT Data Protection Code of**
2 **Conduct**
3 **SAML 2.0 profile**



4 For Service Providers established in European Union, European Economic Area and
5 countries with adequate data protection pursuant to Article 25.6 of the directive 95/46/EC

6 **Version 1.1 DRAFT, 5 August 2014 ~~1.0 Errata 1, 10 June 2014~~**

7 © DANTE on behalf of the GN3plus project. Used under a Creative Commons Attribution ShareAlike license (CC BY-SA 3.0).
8 The work leading to these results has received funding from the European Community's Seventh Framework Programme (FP7 2007–2013)
9 under Grant Agreement No. 605243 (GN3plus).
10

11



12 1. Introduction

13 This profile defines REQUIRED, RECOMMENDED, and OPTIONAL behavior for deployments supporting the
14 Data Protection Code of Conduct. This deployment profile is based on the Organization for the Advancement of
15 Structured Information Standards (OASIS) SAML 2.0 specifications [SAML2 Core, SAML2META]. It also
16 references elements defined in [SAML2MDUI], and makes use of an Entity Category element defined in Entity
17 Category Specification: Data Protection Code of Conduct [CoCEntityCategory]. The requirements from those
18 specifications are not repeated here except where deemed necessary to highlight a point of discussion or draw
19 attention to an issue addressed in errata, but remain implied.

20 This document is supplemented by the non-normative Notes on Implementation of INFORM/CONSENT GUI
21 Interfaces [CoCGUI] document which outlines the current best practice in the implementation and deployment
22 of Identity Provider side modules for attribute release and user consent.

23 Note that the SAML features that are optional, or lack mandatory processing rules, are assumed to be optional
24 and out of scope of this profile if not otherwise precluded or given specific processing rules.

25 The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT",
26 "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

27 2. SAML Metadata Requirements for SP Entities

28 1. mdui Requirements:

- 29 1. SPs MUST provide at least one `mdui:PrivacyStatementURL` value.
- 30 2. It is RECOMMENDED that SPs provide at least one `mdui:DisplayName` value.
- 31 3. It is RECOMMENDED that SPs provide at least one `mdui:Description` value.
- 32 4. For all mdui elements, at least an English version of the element MUST be available, indicated
33 by an `xml:lang="en"` attribute.

34 2. Attribute-related Requirements:

- 35 1. SPs MUST provide `RequestedAttribute` elements describing attributes (and, optionally,
36 requested values) relevant for the SP. The `RequestedAttribute` elements MUST include
37 the optional `isRequired="true"` to indicate that the attribute is necessary.
- 38 2. If the SP requires just one or some particular value(s) of an attribute (such as,
39 `eduPersonAffiliation="member"`), the SP MUST use the `saml:AttributeValue`
40 element to indicate that value(s).
- 41 3. SPs MUST provide an Entity Category attribute [CoCEntityCategory] value asserting compliance with
42 the Code of Conduct.

43 **2.1 Display name**

44 A short descriptive name of the service, if possible without abbreviations. It SHOULD be meaningful both to the
45 users of the service and to readers not affiliated with the service.

46 This value may be displayed by various GUIs in order to identify the service.

47 Examples:

- 48 • Helsinki University's Moodle learning management system
- 49 • University of Tübingen's Weblicht tool for linguistics research

50 **2.2 Description**

51 A description which summarises the service provided. It SHOULD be meaningful both to the users of the
52 service and to readers not affiliated with the service.

53 This value may be displayed by various GUIs in order to summarise the purpose for which the service
54 processes personal data.

55 It is RECOMMENDED that the length of the description is no longer than 140 characters.

56 Examples:

- 57 • SAS-download gives access to SAS®-software for qualified users.
- 58 • bibliotek.dk gives access to all public Danish libraries, and allows users to search for and order
59 materials.
- 60 • WebLicht is a chaining tool for linguistics research. It provides an execution environment for automatic
61 annotation of text corpora.

62 **2.3 Privacy Statement URL**

63 A URL which resolves to a document that is the service's Privacy Policy.

64 This value may be displayed by various GUIs as a clickable link for the end user to provide more information on
65 how the service processes personal data. See Privacy policy guidelines for Service Providers
66 [CoCPrivacyPolicy] for more information.

67 The `PrivacyStatementURL` MUST resolve to a document which is available to browser users without
68 requiring authentication of any kind.

69 2.4 Requested Attribute

70 Zero or more elements specifying attributes and, when applicable, attribute values requested by this service.
71 Having no `RequestedAttribute` element in place implies the service does not request any attributes.

72 If the Service Provider supports both SAML 1.x and SAML 2.0 protocols, it SHOULD list requested attributes
73 using only the SAML 2.0 attribute naming conventions [`MACEDirAttrProf`].

- 74 • Note: The underlying SAML 2.0 metadata standard is unable to express the attribute requirements of
75 such a Service Provider. The recommendation above is intended to minimise the chance of
76 interoperability problems arising. It is further RECOMMENDED that such a Service Provider uses the
77 SAML 2.0 protocol when possible rather than SAML 1.x.

78 A necessary attribute is indicated using the `isRequired="true"` XML attribute. In the context of this Data
79 protection Code of Conduct, an attribute is required only if it is both relevant and necessary for enabling access
80 to the service.

81 `isRequired="false"` or a missing `isRequired` XML attribute indicates the attribute is optional (relevant,
82 but only useful or desirable).

83 See What attributes are relevant for a Service Provider [`CoCAttributes`] document for assistance on the
84 necessary and optional attributes. See also Data protection good practice for Home Organisations
85 [`CoCHomeOrg`] document for a good practice on managing the release of attributes flagged as necessary or
86 optional.

87 Note: Introduction to Code of Conduct [`CoCIntroduction`] proposes to defer the support to attributes flagged as
88 optional to Phase 2.

89 2.5 Entity Category: Data protection Code of Conduct

90 An Entity Category attribute as defined in the Entity Category Specification: Data Protection Code of Conduct
91 [`CoCEntityCategory`].

92 3. SAML Metadata Requirements for IDP Entities

93 IdPs MUST provide an Entity Category support attribute [`CoCEntityCategory`] value asserting that they are
94 willing to interact with Service Providers conforming to the Code of Conduct.

95 ~~Currently, there are no metadata requirements for IDPs.~~

96 4. Examples

97 Only related elements and attributes are presented.

98 Example (Service Provider):

```

99 <EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" entityID="https://filesender.example.org/">
100   <Extensions>
101     <EntityAttributes xmlns="urn:oasis:names:tc:SAML:metadata:attribute">
102       <Attribute xmlns="urn:oasis:names:tc:SAML:2.0:assertion"
103         Name="http://macedir.org/entity-category"
104         NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format-uri">
105         <AttributeValue>http://www.geant.net/uri/dataprotection-code-of-conduct/v1</AttributeValue>
106       </Attribute>
107     </EntityAttributes>
108   </Extensions>
109   <SPSSODescriptor>
110     <Extensions>
111       <UIInfo xmlns="urn:oasis:names:tc:SAML:metadata:ui">
112         <DisplayName xml:lang="fi">FileSender</DisplayName>
113         <DisplayName xml:lang="en">FileSender</DisplayName>
114         <Description xml:lang="fi">FileSender tarjoaa helpon tavan jakaa suuria tiedostoja.</Description>
115         <Description xml:lang="en">FileSender offers an easy way to share large files with anyone.</Description>
116         <PrivacyStatementURL xml:lang="fi">https://filesender.example.org/privacy-fi.html</PrivacyStatementURL>
117         <PrivacyStatementURL xml:lang="en">https://filesender.example.org/privacy-en.html</PrivacyStatementURL>
118       </UIInfo>
119     </Extensions>
120     <AttributeConsumingService>
121       <RequestedAttribute
122         FriendlyName="displayName"
123         Name="urn:oid:2.16.840.1.113730.3.1.241"
124         NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format-uri"
125         isRequired="true"/>
126       <RequestedAttribute
127         FriendlyName="eduPersonPrincipalName"
128         Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6"
129         NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format-uri"
130         isRequired="true"/>
131       <RequestedAttribute
132         FriendlyName="mail"
133         Name="urn:oid:0.9.2342.19200300.100.1.3"
134         NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format-uri"
135         isRequired="true"/>
136     </AttributeConsumingService>
137   </SPSSODescriptor>
138 </EntityDescriptor>
139

```

140 Example (Identity Provider):

```

141 <EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" entityID="https://idp.example.org/">
142   <Extensions>
143     <EntityAttributes xmlns="urn:oasis:names:tc:SAML:metadata:attribute">
144       <Attribute xmlns="urn:oasis:names:tc:SAML:2.0:assertion"
145         Name="http://macedir.org/entity-category-support"
146         NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
147         <AttributeValue>http://www.geant.net/uri/dataprotection-code-of-conduct/v1</AttributeValue>
148       </Attribute>
149     </EntityAttributes>
150   </Extensions>
151 </EntityDescriptor>

```

152 **References**

| | | |
|-----|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 153 | [CoCAAttributes] | Data protection Code of Conduct, "What Attributes Are Relevant for a Service Provider", < https://refeds.terena.org/index.php/What_attributes_are_relevant_for_a_Service_Provider > |
| 154 | [CoCEntityCategory] | Data protection Code of Conduct, "Entity Category Specification", Version 1.1, 5 August 2014 1.0, 14 June 2013 |
| 155 | [CoCGUI] | Data protection Code of Conduct, "Notes on Implementation of INFORM/CONSENT GUI Interfaces", < https://refeds.terena.org/index.php/Notes_on_Implementation_of_INFORM/CONSENT_GUI_Interfaces > |
| 156 | [CoCHomeOrg] | Data protection Code of Conduct, "Data Protection Good Practice for Home Organisations", < https://refeds.terena.org/index.php/Data_protection_good_practice_for_Home_Organisations > |
| 157 | [CoCIntroduction] | Data protection Code of Conduct, "Introduction to Code of Conduct", < https://refeds.terena.org/index.php/Introduction_to_Code_of_Conduct > |
| 158 | [CoCPrivacyPolicy] | Data protection Code of Conduct, "Privacy Policy Guidelines for Service Providers", < https://refeds.terena.org/index.php/Privacy_policy_guidelines_for_Service_Providers > |
| 159 | [MACEDirAttrProf] | MACE-Dir, "SAML Attribute Profiles", April 2008. |
| 160 | [SAML2 Core] | OASIS, "Assertions and Protocol for the OASIS Security Markup Language (SAML) V2.0", , 15 March 2005. Document Identifier: saml-core-2.0-os, < http://docs.oasis- open.org/security/saml/v2.0/saml-core-2.0-os.pdf > |
| 161 | [SAML2META] | Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0 , with various addenda, and in associated specifications. |
| 162 | [SAML2MDUI] | SAML V2.0 Metadata Extensions for Login and Discovery User Interface Version 1.0. |
| 163 | | |
| 164 | | |
| 165 | | |
| 166 | | |
| 167 | | |
| 168 | | |
| 169 | | |
| 170 | | |
| 171 | | |
| 172 | | |
| 173 | | |
| 174 | | |

175

Document History

176

Changes from Version 1.0 Erreta 1, 10 June 2014

177

- Introduced a mandatory Entity Category support attribute for Identity Providers.

178

179

Changes from Version 1.0, 14 June 2013

180

- Removed white space characters from the <AttributeValue>, <mdui:DisplayName>, <mdui:Description> and <mdui:PrivacyStatementURL> elements in the Examples section and reformatted the example.

181